

ABSTRACT OF THE DISCLOSURE

An apparatus authentication system that includes a server apparatus and a client apparatus which perform a mutual authentication when a content is transmitted from the server apparatus to the client apparatus for use. The client apparatus receives challenge data from the server apparatus, generates signature data based on the received challenge data and a first password, and transmits the generated signature data. The server apparatus generates and transmits the challenge data, holds a second password in advance, receives the signature data from the client apparatus, performs an authentication of the received signature data using the challenge data and the second password, and if the authentication results in success, transmits an encrypted content to the client apparatus.